View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Northwestern University Illinois, School of Law: Scholarly Commons

Northwestern Journal of Technology and Intellectual Property

Volume 13 | Issue 1 Article 4

2015

You're Fired: Pack Everything but Your Social Media Passwords

Hugh McLaughlin
Northwestern University School of Law

Recommended Citation

Hugh McLaughlin, *You're Fired: Pack Everything but Your Social Media Passwords*, 13 Nw. J. Tech. & Intell. Prop. 87 (2015).
https://scholarlycommons.law.northwestern.edu/njtip/vol13/iss1/4

This Comment is brought to you for free and open access by Northwestern Pritzker School of Law Scholarly Commons. It has been accepted for inclusion in Northwestern Journal of Technology and Intellectual Property by an authorized editor of Northwestern Pritzker School of Law Scholarly Commons.

N O R T H W E S T E R N
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

You're Fired: Pack Everything but Your Social Media Passwords

Hugh McLaughlin

February 2015 VOL. 13, NO. 1

© 2015 by Northwestern University School of Law
Northwestern Journal of Technology and Intellectual Property

Copyright 2015 by Northwestern University School of Law
Northwestern Journal of Technology and Intellectual Property
Volume 13, Number 1 (February 2015)

You're Fired: Pack Everything but Your Social Media Passwords

By Hugh McLaughlin*

The global proliferation of social media has transformed these online platforms—once used almost exclusively by young, tech-savvy Millennials—into transcontinental mediums of communication and expression. Through social media, dictatorships have been overthrown, human rights abuses have been exposed, and the oppressed have been given a voice. The social and cultural impact has been truly prolific. But until recently, social media's economic impact was less clear. Now, though, myriad evidence—ranging from studies focusing on revenue generated from a single Facebook "Like," to commentary positing that trillions of dollars in value have yet to be realized—indicates the potential commercial advantages stemming from social media's use. With over one-billion users worldwide, the small percentage of companies not using social media to market and maintain relationships will likely face difficulty competing with companies that adequately utilize these inexpensive platforms.

But while social media's place in commerce is now established, the legal consequences of its misuse in the workplace are nebulous. Courts and legislatures have struggled to balance the competing interests of business autonomy and employees' privacy rights, ultimately resulting in a patchwork of judicial holdings and reactive legislation. And with little guidance from courts, companies have struggled to adapt to the ever-changing social media landscape. Thus, companies are attempting to navigate the legal thicket by drafting explicitly restrictive social media policies that protect business interests.

This legal ambiguity has prompted a recent trend in employment-contract drafting that threatens to disrupt social media's market potential. These new provisions effectively force employees to turn over social media passwords to their employers upon termination of employment. At first blush, this practice might seem innocuous. This Comment argues that it is anything but. Coupled with a balancing of the equities approach, an analysis of pertinent principles of contract, privacy, and tort law shows that employees' rights should prevail. As a matter of law and equity, an employee's right to retain access to her social media accounts post-termination should be assured through a judicial prohibition of these overly intrusive employment provisions.

---

* Candidate for Juris Doctor, 2015, Northwestern University School of Law. Editor-in-Chief, Northwestern Journal of Technology and Intellectual Property. I'd like to express my deepest gratitude to the Northwestern Journal of Technology and Intellectual Property, with a special thanks to Justin Morgan, Rachel Stigler, Natasha Chu, Sean Apfelbaum, Andrew Thompson, Tricia Dickson, Christie Cho, Paul Barrus, Corey Berkin, C. Dylan Turner, Ryan Timmis, Amy Garber, and Jonathon Studer for all of their hard work and thoughtful contributions.

TABLE OF CONTENTS

INTRODUCTION

¶1 The global proliferation of social media has transformed these online platforms—once used almost exclusively by young, tech-savvy Millennials[1]—into transcontinental mediums of communication and expression. Through social media, dictatorships have been overthrown,[2] human rights abuses have been exposed,[3] and the oppressed have been given a voice.[4] The social and cultural impact has been truly prolific. But until recently, social media's economic impact was less clear. Now, though, myriad evidence—ranging

[1] For example, Facebook initially required a Harvard.edu email address. Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, & Scholarship*, 13 J. OF COMPUTER-MEDIATED COMM. 210, 218 (2008).

[2] *See* Catherine O'Donnell, *New Study Quantifies Use of Social Media in Arab Spring*, UNIV. OF WASH. (Sept. 12, 2011), http://www.washington.edu/news/2011/09/12/new-study-quantifies-use-of-social-media-in-arab-spring/.

[3] *See* Christoph Koettl, *Twitter to the Rescue? How Social Media Is Transforming Human Rights Monitoring*, HUMAN RIGHTS NOW BLOG (Feb. 20, 2013, 4:34 PM), http://blog.amnestyusa.org/middle-east/twitter-to-the-rescue-how-social-media-is-transforming-human-rights-monitoring/.

[4] *See* Phelim Kine, *Chinese Government's Oppressive Policies Draw Ire from the Public*, HUMAN RIGHTS WATCH (Aug. 3, 2012), http://www.hrw.org/news/2012/08/03/chinese-governments-oppressive-policies-draw-ire-public.

from studies focusing on revenue generated from a single Facebook "Like,"[5] to commentary positing that trillions of dollars in value have yet to be realized[6]—indicates the potential commercial advantages stemming from social media's use. With over one-billion users worldwide, the small percentage of companies not using social networking services (SNSs), such as LinkedIn, Facebook, and Twitter, to market and maintain relationships will face difficulty competing with companies that adequately utilize these inexpensive platforms.[7]

¶2 However, a recent trend in employment-contract drafting threatens to disrupt social media's market potential. These new provisions effectively force employees to turn over social media passwords to their employers upon termination of employment.[8] In other words, these restrictive social media policies compel employees to assign their social media access rights to the company. At first blush, this practice might seem innocuous. This Comment argues that it is anything but. Coupled with a balancing of the equities approach, an analysis of pertinent principles of contract, privacy, and tort law shows that employees' rights should prevail. As a matter of law and equity, an employee's right to retain access to her social media account post-termination should be ensured through a judicial prohibition of these overly intrusive employment provisions.

¶3 Because it is important to understand the uneasy intersection of law and social media, this Comment begins with a basic overview. Part I addresses the unclear legal landscape regarding social media in the workplace and analyzes the importance of social media's use to employees generally. Part II begins the substantive argument looking to the most prominent SNSs—Facebook, Twitter, and LinkedIn—and the similar contractual provisions in their user agreements specifically defining this employment practice as a breach of contract. However, because courts have suggested that employers may assert legal ownership over individual employee accounts, Part III addresses the most relevant case, *Eagle v. Morgan*,[9] delving into the court's reasoning and pertinent dicta. Part IV analyzes the suitability of privacy law protection in *Eagle* and generally. Part V discusses the inherently public nature of social media and the inapplicability of trade-secret law. Part VI analyzes the judicial and legislative trends favoring employee social media rights. Finally, Part VII offers a socioeconomic justification addressing the actual and potential value of social media, and how this should impact judicial analysis and SNS decision-making.

¶4 Recognizing that no legal principle adequately addresses the alienability of social media accounts in the workplace, this Comment provides a roadmap for courts to balance

---

[5] *See* Jim Edwards, *What Is a Facebook "Like" Actually Worth in Dollars*, BUS. INSIDER (Mar. 27, 2013), http://www.businessinsider.com/what-is-a-facebook-like-actually-worth-in-dollars-2013-3 (citing multiple studies focusing on the value of Facebook "Likes").

[6] *See* MICHAEL CHUI ET AL., MCKINSEY INST., THE SOCIAL ECONOMY: UNLOCKING VALUE AND PRODUCTIVITY THROUGH SOCIAL TECHNOLOGIES 9 (2012) [hereinafter SOCIAL ECONOMY], *available at* http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_social_economy.

[7] *See id.* at 51.

[8] *See, e.g.,* Eagle v. Morgan, Civil Action No. 11–4303, 2013 WL 943350 (E.D. Pa. Mar. 12, 2013). See Jennifer L. Parent, *Advising Clients on Today's Top Employment Law Issues*, ASPATORE, Feb. 2013, at 5, and Sara Hutchins Jodka, *Arm Yourself: Battle over Social Media Account Ownership Has Begun*, 23 OHIO. EMP. L. LETTER, Oct. 2012, at 1, for discussions suggesting employers draft and implement employment policies asserting company ownership over employee social media accounts.

[9] *Eagle*, 2013 WL 943350.

the equities, along with a supplemental call-to-arms for SNS intervention. Taking into account the factors outlined *infra*, the equitable scale of justice weighs in favor of a judge-made rule prohibiting the enforcement of employment provisions that assert company ownership over employee social media accounts.

I. BACKGROUND OF SOCIAL MEDIA AND THE LAW

¶5 It is now easier than ever to expand one's professional network, maintain relationships, and communicate instantly.[10] Over 72% of companies use social media, and one study estimates that the global economy has yet to realize trillions of dollars in value created by social media's use.[11] Even assuming a more conservative valuation, capable parties will undoubtedly seek out ways to maximize gains before others attempt the same. Thus, social media's eventual value may not depend primarily upon overall usage, but rather upon which parties are best able to capture its current, unrealized economic potential.[12]

¶6 On the other hand, social media platforms are inherently interpersonal. They are "social" after all. They give people an avenue to express their thoughts freely, share personal experiences with loved ones, and revitalize long-lost friendships. A truly global community now exists due to social media's proliferation.

¶7 Problems arise, though, when seemingly temporary communication becomes permanent, or when the ease of usage allows someone to do something in the heat of a moment that he later regrets.[13] Further, the often-blurred line between the "social" aspects of social media and its professional use in the workplace exacerbates these issues.[14]

¶8 While social media's place in commerce is now established,[15] the legal consequences of its misuse are nebulous. With little guidance from courts, companies have struggled to adapt to the ever-changing social media landscape.[16] From screening job applicants' Facebook profiles,[17] to combatting trade-secret theft by ex-employees,[18]

---

[10] *See* Robert Ball, *Social Media Marketing: What's the Payoff for Your Business*, HUFFINGTON POST (Feb. 24, 2011, 6:00 PM), http://www.huffingtonpost.com/robert-ball/do-you-know-how-social-me_b_826802.html.

[11] *See* SOCIAL ECONOMY, *supra* note 6.

[12] While over a billion Internet users frequent social media websites, the unrealized financial growth supports the proposition that total usage statistics may not accurately gauge social media's current value. *See id.*; *see cf*. Ken Strutin, *Social Media and the Vanishing Points of Ethical and Constitutional Boundaries*, 31 PACE L. REV. 228, 237 (2011) (describing social media's use in prison in that "the value of a communication/information source is measured by the need to control access to it").

[13] *See* Jennifer L. Naeger, *United States: Effectively Managing Social Media in the Workplace,* MONDAQ (May 15, 2013), http://www.mondaq.com/unitedstates/x/239152/employee+rights+labour+relations/EFFECTIVELY+MANAGING+SOCIAL+MEDIA+IN+THE+WORKPLACE.

[14] *See id.*; Jodka, *supra* note 8.

[15] *See* SOCIAL ECONOMY, *supra* note 6.

[16] *See* John Balitis, Jr. & Carrie Pixler Ryerson, *Social Media's Lessons*, 48 ARIZ. ATT'Y 17, 17 (Apr. 2012) ("In 2012, as more and more employers are using social media for their own gain, a new controversy has emerged. Employers now are embroiled in litigation against former employees over the issue of who owns social media pages and accounts: the employer or the employee.").

[17] *See* Sara E. Stratton, Note, *Passwords Please: Rethinking the Constitutional Right to Informational Privacy in the Context of Social Media*, 41 HASTINGS CONST. L.Q. 649, 649 (2014).

[18] *E.g.,* Phonedog v. Kravitz, No. C 11–03474 MEJ., 2011 WL 5415612, at *6 (N.D. Cal. Nov. 8, 2011); *see* 5A RICHARD A. ROSS, METHODS OF PRACTICE, MINN. PRAC. § 4.50.10(A) (Roger S. Haydock & Peter

companies are attempting to navigate the legal thicket by drafting social media policies that protect business interests without violating civil liberties[19] or damaging employee morale.[20] Similarly, courts and legislatures have struggled to balance the competing interests of business autonomy and employees' privacy rights, ultimately resulting in a patchwork of judicial holdings and reactive legislation.

¶9 Social media's rapid expansion in the workplace has left courts and legislatures attempting to cope with a myriad of disputes.[21] In many ways, this new technology has transformed once-settled areas of law into quagmires of inconsistent precedent.[22] In light of this confusion, commentators suggest that companies should draft explicitly restrictive social media policies to protect business interests.[23]

¶10 Governing bodies have attempted to provide guidance through legislation. For instance, the National Labor Relations Act protects certain employee privacy rights on social media,[24] while multiple states have statutorily banned companies from asking employees for social media passwords.[25] Although statutes and agency regulations have provided some direction for corporate governance, companies are still searching for answers that often do not exist. Ultimately, the judiciary needs to find a way to rectify these issues consistently.

¶11 Unfortunately, few courts have been able to provide much clarity. The way courts have decided many of these issues has been at best inconsistent and at worst incoherent. Often judges seem to shove square pegs into round holes, relying on statutes like the Computer Fraud and Abuse Act (CFAA), drafted nearly three decades ago, to justify decisions concerning an issue never contemplated by the drafters of such legislation.[26] In

---

B. Knapp eds., 4th ed. 2013); Jodka, *supra* note 8.

[19] *See* ROSS, *supra* note 18; Kathy Ossian, *Protecting Sensitive Information in Cyberspace: Recent Trends and Recommended Strategies*, ASPATORE, Aug. 2013, at 1.

[20] *See* Mickie Kennedy*, The Case Against Creating a Corporate Social Media Policy*, ERELEASES, http://www.ereleases.com/prfuel/against-creating-corporate-social-media-policy (last visited Sept. 18, 2014).

[21] *See* Michael Masri & Pedram Tabibi, *Social Media at Work Raises Issues of Account Ownership*, N.Y.L.J., Mar. 26, 2012, at 11–12.

[22] *See* Ashley Kasarjian, *The Social Media Checklist for Companies: What Your Clients Should Do, Know and Learn*, 49 ARIZ. ATT'Y 16 (Mar. 2013).

[23] *See, e.g., id.*; Masri & Tabibi, *supra* note 21, at 12; Bethany N. Whitfield, Comment, *Social Media @ Work: #POLICYNEEDED*, 66 ARK. L. REV. 843, 847 (2013) (citing Maureen Minehan, *Protect Social Media Assets from Departing Employees*, EMP. ALERT, Mar. 21, 2012, at 1, *available at* http://www.dinsmore.com/files/upload/socialmediaassets.pdf).

[24] *See* Kasarjian, *supra* note 22, at 18 (citing NAT'L LABOR RELATIONS BD., REPORT OF THE ACTING GENERAL COUNSEL CONCERNING SOCIAL MEDIA CASES (2012), *available at* http://www.nlrb.gov/news-outreach/news-story/acting-general-counsel-releases-report-employer-social-media-policies).

[25] *See id.*

[26] 18 U.S.C. § 1030(g); *see, e.g.,* Eagle v. Morgan, Civil Action No. 11–4303, 2012 WL 4739436, at *5 (E.D. Pa. Oct. 4, 2012), *aff'd*, Eagle v. Morgan, Civil Action No. 11–4303, 2013 WL 943350 (E.D. Pa. Mar. 12, 2013) (holding that damages under the CFAA must result from actual loss, not potential business opportunities); P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, 428 F.3d 504 (3d Cir. 2005); *see also* Andrew T. Hernacki, *A Vague Law in a Smartphone World: Limiting the Scope of Unauthorized Access Under the Computer Fraud and Abuse Act*, 61 AM. U. L. REV. 1543, 1547 (2012) (arguing, *inter alia*, that an overly broad application of the CFAA is unconstitutionally vague, thus its scope should be limited to the original legislative goal of it being an "anti-hacking" statute).

this same vein, an overreliance on intellectual property law[27] and state common-law doctrines has led to similar vagaries.[28]

¶12 These holdings are as unpredictable as they are confusing. Simply put, there are very few standards dealing with social media rights in the workplace for courts to rely upon. Even less guidance exists to help companies shape viable social media policies.[29] Due to this lack of clarity, disputes between employers and employees have been numerous and incredibly varied.[30]

¶13 Moreover, when courts have confronted social media disputes in the workplace, the inquiries have been excessively fact-intensive.[31] Realistically, no cure-all likely exists for the multitude of issues faced. While the task is daunting, only a piecemeal process addressing specific scenarios related to social media in the workplace appears to offer adequate, albeit meticulous, remedies. Thus, this Comment addresses the narrow issue of whether courts should enforce employment contracts that mandate the transfer of individual, employee-created social media accounts upon termination.

¶14 These ownership rights are crucial for the ex-employee because often the only contact information for individuals in a professional network is stored within these social media accounts.[32] Furthermore, even if an individual is able to collect the information

---

[27] These forced-transfer provisions allow companies to replace the former employee's account information with a new company representative's information. Thus, the resulting "likelihood of confusion" would realistically be minimal because "there is no comparison between two competing goods" (e.g., the different profile identities). *Eagle*, 2012 WL 4739436, at *7. The only way a trademark violation under the Lanham Act would occur is if the company neglected to change the profile information, and subsequently attempted to "pass off" the new account holder as the former employee. *Id.* Since this Comment focuses on access rights to social media accounts and the insertion of a new, company-appointed representative, the implications of trademark or copyright protection are less applicable.

[28] *See, e.g., Eagle*, 2013 WL 943350, at *10 (discussing how the elements of conversion differ across states, and specifically that Pennsylvania does not recognize conversion for intangible chattels, thus barring plaintiff's claim). *See* Tiffany A. Miao, *Access Denied: How Social Media Accounts Fall Outside the Scope of Intellectual Property Law and into the Realm of the Computer Fraud and Abuse Act*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1017 (2013).

[29] *See* Steve Cosentino, *Contracting and Compliance in a Web of Data Security Regulations*, ASPATORE, Mar. 2013, at 1 ("Unfortunately, because there is no central authority for these issues, lawyers must wade through a tangled mess of laws, regulations, and standards to provide effective counsel to our clients.").

[30] *See* Scott Brutocao, *Issue Spotting: The Multitude of Ways Social Media Impacts Employment Law and Litigation*, 60 THE ADVOC. 8, 8 (2012) (describing the various issues faced in the employment context dealing with social media); *see also* ROSS, *supra* note 18, ¶ (B) (citations omitted) ("In addition to considering social media policies, through the Internet, employers can learn information about employees and potential employees that can give rise to myriad claims including: off-duty conduct claims, retaliation claims, discrimination claims, or whistleblower claims.").

[31] *See* Joshua A. Mooney, *Locked out on LinkedIn: LinkedIn Account Belongs to Employee, Not Employer*, 25 INTELL. PROP. & TECH. L.J. 16, 18 (2013) ("The ultimate merit of such claims will be fact intensive.").

[32] For example, in *Eagle*:

> For many contacts, LinkedIn was the best way to keep in touch with them, particularly because Eagle's only email address on the account was her Edcomm address. . . . Eagle was powerless to control how the LinkedIn account was being used; . . . [she] has still been unable to respond to messages that were sent to the account. . . . [She] missed out on professional opportunities by being unable to respond to these messages.

Eagle, 2012 WL 4739436, at *4.

before leaving a company, establishing a new network is cumbersome, imperfect, and ultimately deleterious to both the employee and the professional network.[33]

¶15 It is relatively clear that an ex-employee retains access rights to her individual, password-protected account if the former employee created the account prior to gaining such employment and the company has no explicit social media policy in place.[34] However, the question becomes more difficult when the company has an employment policy mandating specific terms of social media usage, or perhaps, an employee creates a personal social media account at the company's direction.[35] These policies might mandate the creation of individual social media accounts, dictate the content contained within profiles, outline suitable information for employees to post or share, and most importantly for this Comment, assert company ownership of a social media account upon termination of employment.[36] If both dicta in the most relevant case, *Eagle v. Morgan*,[37] and recent commentary are any indicator,[38] these restrictive social media policies will become increasingly common.

---

[33] *See* Charles Caro, Comment to *How Do I Create a Second Account*, LINKEDIN (Aug. 10, 2013, 4:31 PM), http://community.linkedin.com/questions/79023/how-do-i-create-a-second-account.html (describing provisions of LinkedIn's User Agreement not allowing second accounts to be created, and that duplicating accounts is not beneficial due to "the nature of social networking"); Alisa Meredith, *How to Recover Your Facebook Business Page from Rogue or Clueless Employees*, SCALABLE SOC. MEDIA BLOG (Feb. 7, 2013), http://scalablesocialmedia.com/2013/02/recover-facebook-page/ (addressing the difficulties associated with recovering information from no-longer-accessible social media accounts); *see also* Stephanie Sammons, *4 Tips for Improving Your Social Media Presence in 2014*, WIRED ADVISOR, http://blog.wiredadvisor.com/how-to-improve-your-social-media-presence/ (last visited Aug. 26, 2014); *infra* text accompanying notes 179–91 (analyzing argument pointing to possibility of over-commercialization adversely affecting invaluable community building aspects of social media).

[34] Whitfield, *supra* note 23, at 847 (citing Maureen Minehan, *Protect Social Media Assets from Departing Employees*, EMP. ALERT, Mar. 21, 2012, at 1); *see, e.g.,* Eagle v. Morgan, Civil Action No. 11–4303, 2013 WL 943350 (E.D. Pa. Mar. 12, 2013).

[35] *See, e.g., Eagle*, 2013 WL 943350; *see* Parent, *supra* note 8; Masri & Tabibi, *supra* note 21, at 12.

[36] *See* Parent, *supra* note 8; Masri & Tabibi, *supra* note 21, at 12.

[37] Edcomm's counterclaim for misappropriation failed but for certain factors:

> Edcomm never had a policy of requiring that its employees use LinkedIn, did not dictate the precise contents of an employee's LinkedIn account, and did not pay for its employees' LinkedIn accounts. Indeed, as noted above, the LinkedIn User Agreement expressly states that Plaintiff's account is between LinkedIn and the individual user. Edcomm did not itself maintain any separate account. Moreover, Edcomm failed to put forth any evidence that Eagle's contacts list was developed and built through the investment of Edcomm time and money as opposed to Eagle's own time, money, and extensive past experience. Accordingly, the Court finds in favor of Eagle on this claim.

Eagle, 2013 WL 943350, at *16.

[38] *See* Kasarjian, *supra* note 22, at 20 (referring to *Eagle*, author suggests that employers should draft specific contracts and company policies because "[i]t is important to note at the outset who owns and has a right to view/use information, communications, and even accounts—such as LinkedIn" to best avoid litigation); Jodka, *supra* note 8 (suggesting companies draft clear corporate policies that assert ownership over all social media accounts used in relation to employment and that employee access will cease upon termination); *cf.* City of Ontario, Cal. v. Quan, 560 U.S. 746, 758–59 (2010) (asserting employer's computer policy and "operational realities" determined employee's reasonable expectation of privacy, thus limiting Fourth Amendment protection).

¶16 This Comment argues that courts should adopt an exclusive rule prohibiting the forced transfer of employee social media accounts via employment contracts upon termination. This ban should apply only to individual-member accounts created in an employee's own name, not to public profiles created in the name of the company, such as a "Facebook Page."[39] This restriction should apply categorically to all individual-user accounts, regardless of whether an employee created the account before or after employment commenced, or if the employer paid for an account upgrade. Finally, this rule should only protect the employee's *access rights* to the account and professional network. Any content belonging to the company within the profile should still be subject to existing valid rights, such as copyright and trademark protection.

¶17 Further, while state or federal legislation prohibiting these forced-transfer provisions might seem sufficient, the judiciary's inherent equity powers provide the necessary flexibility and autonomy for reaching the most suitable result. With respect to new technology, legislatures are often ill equipped to provide adequate solutions in an ever-changing innovative environment. Additionally, while lawmakers might legitimately desire a ban on forced-transfer provisions, the inevitable intervention of big-business lobbyists supporting a company's right to draft and enforce these provisions might cause some politicians to balk at election time, or in the alternative, lead to watered-down, ineffective legislation. Either way, the judiciary stands as the most capable body for finding a solution in this context.

¶18 This Comment first argues that the textual conflict between these restrictive employment contracts and the most common SNS user agreements should prompt a finding that the former are facially invalid. However, although these forced-transfer provisions appear patently impermissible, courts addressing this issue have suggested otherwise if employees assign away their access rights.[40] Thus, an analysis will follow suggesting that if social media ownership rights do in fact exist in the employment context, then these rights are inalienable and exclusively belong to the employee. Lastly, the potential adverse economic and social consequences, considered in the aggregate, should both bolster the justification for an exclusive judicial rule prohibiting forced-transfer employment provisions and prompt SNSs to similarly oppose these agreements.

II. OWNERSHIP RIGHTS IN SOCIAL MEDIA: CONFLICTING CONTRACTS

¶19 "The word 'owner' . . . means the person who has one or more interests."[41] Additionally, the term "interest" includes "a right, power, privilege, or immunity or any two or more of these things."[42] Thus, the employer, employee, and SNS could assert social media ownership rights concurrently. In other words, multiple parties may acquire valid rights to different aspects of a single social media account.[43]

---

[39] *See Page Guidelines*, FACEBOOK, https://www.facebook.com/page_guidelines.php (last visited Sept. 16, 2014).

[40] *See, e.g., Eagle*, 2013 WL 943350, at *16.

[41] RESTATEMENT (FIRST) OF PROP. § 10 (1936).

[42] *Id.*

[43] *See, e.g., Help Center*, LINKEDIN, http://help.linkedin.com/app/answers/detail/a_id/4783/ft/eng (last visited Aug. 25, 2014) ("If you're an administrator, you can: [a]dd other administrators [and] [e]dit your Company Page.").

¶20 But the proper assignment of these rights can be less clear. Courts have struggled to identify which party should have the right to access a social media account when multiple parties assert contractual access rights.[44] However, a textual examination of SNS user agreements makes allocating these rights less problematic.

¶21 Although specific terms vary, the most common SNS user agreements contain nearly identical substantive provisions. For instance, SNSs invariably retain the right to terminate accounts at their sole discretion. Twitter's Terms of Service state, "We reserve the right at all times . . . to suspend or terminate users, and to reclaim usernames."[45] Similarly, "[LinkedIn] may modify, replace, refuse access to, suspend or discontinue LinkedIn . . . for all our Members in [its] sole discretion."[46] Thus in reality, neither employer nor employee can claim to be the true owner of a social media account since the SNS may end the agreement at any time.[47]

¶22 The SNS grants a revocable license to use the service.[48] LinkedIn's User Agreement makes it clear that "between you and others, your account belongs to you."[49] After an employee agrees to these licensing terms, the employee's right to access the account is superior to all but the true owner's right—the SNS. Moreover, specific provisions define the employee as the licensee, not the company: "If you are using LinkedIn on behalf of a company or other legal entity, you are nevertheless individually bound by this Agreement even if your company has a separate agreement with us."[50] In other words, the agreement is between only the SNS and the individual setting up the account, not the company.

¶23 Importantly, these SNS agreements explicitly forbid transferring accounts, sharing passwords, and impersonating others, even with permission.[51] LinkedIn requires that a user "not permit others to use [the] account . . . use other's accounts . . . [and] not sell, trade, or *transfer* [a] LinkedIn account to another party."[52] Similarly, Facebook's Terms of Service state, "You will not share your password . . . let anyone else access your account . . . [or] transfer your account to anyone without first getting our written

---

[44] *See, e.g., Eagle*, 2013 WL 943350, at *16; Phonedog v. Kravitz, No. C 11–03474 MEJ., 2011 WL 5415612 (N.D. Cal. Nov. 8, 2011).

[45] *Terms of Service*, TWITTER, https://twitter.com/tos (last visited Aug. 25, 2014) [hereinafter *Twitter Terms*].

[46] *User Agreement,* LINKEDIN, http//www.LinkedIn.com/legal/user-agreement (last visited Aug. 25, 2014) [hereinafter *LinkedIn Agreement*].

[47] *See Twitter Terms*, *supra* note 45.

[48] *Id.*; *see* ALI PRINCIPLES OF INTELL. PROP. § 315 (Proposed Final Draft 2007).

[49] *LinkedIn Agreement*, *supra* note 46.

[50] *Id*.

[51] *See id.* ("[Y]ou grant LinkedIn a nonexclusive, irrevocable, worldwide, perpetual, unlimited, assignable, sublicensable, fully paid up royalty-free right to us to copy, prepare derivative works of, improve, distribute, publish, remove, retain, add, process, analyze, use and commercialize . . . any information you provide."); *Statement of Rights and Responsibilities*, FACEBOOK, https://www.face book.com/legal/terms (last visited Aug. 25, 2014) [hereinafter *Facebook Agreement*]; *Twitter Terms*, *supra* note 45.

[52] *LinkedIn Agreement*, *supra* note 46 (emphasis added). "If you are using LinkedIn on behalf of a company or other legal entity, you are nevertheless individually bound by this Agreement even if your company has a separate agreement with us." *Id*. *See Facebook Agreement*, *supra* note 51; *Twitter Terms*, *supra* note 45.

permission."[53] Therefore, these agreements not only grant members the right to exclude others from an account, but also require members to make every effort to maintain exclusive access to that account. Simply put, exclusive access is both a right and a contractual obligation.

¶24 LinkedIn and Facebook do not allow non-natural persons (e.g., corporations) to have individual-member accounts. It is a violation of Facebook's Statement of Rights and Responsibilities to "[c]reate a [m]ember profile for anyone other than a natural person," and while "an employee [may] create a page for a company . . . specific parameters" must be met.[54] For instance, the "Company Page" must be public.[55] LinkedIn allows something similar for a company wishing to promote and market itself, along with analogous parameters for the company's use of the service.[56] LinkedIn and Facebook clearly differentiate between individual and company accounts, and have entirely separate agreements for the two.

¶25 In addition, the mere assertion of company ownership may violate various SNS policies. Facebook's Statement of Rights and Responsibilities states, "You will not facilitate or encourage any violations of this Statement or our policies,"[57] and its Non-Solicitation Policy states, "You will not solicit login information or access an account belonging to someone else."[58] Moreover, when a company seizes control of an ex-employee's account, the ex-employee's connections never agreed to be part of the new user's network, which contradicts Facebook's policy that "[Facebook] will only process name changes . . . that do not result in a misleading or unintended connection."[59] Further, LinkedIn requires members to access only their accounts, keep all passwords confidential, and not impersonate others,[60] and forbids uploading anything that "[f]alsely states, impersonates or otherwise misrepresents your identity."[61] Twitter's Impersonation Policy likewise forbids "portraying another person in a confusing or deceptive manner."[62] Thus, in many ways, even if a company decides not to seize control of an employee's account upon termination, the forced-transfer provision itself still violates, either directly or indirectly, the most prominent SNS user agreements.

¶26 Stated simply, SNS user agreements grant inalienable licenses for individual account access. Yet, while these provisions are seemingly unambiguous, courts have either conducted only cursory analysis of the SNS user agreements or simply neglected to enforce them.[63] Even after acknowledging these contractual prohibitions, courts have

---

[53] *Facebook Agreement*, *supra* note 51.

[54] *Id*.

[55] *See id.*

[56] *See Page Guidelines*, FACEBOOK, https://www.facebook.com/page_guidelines.php (last visited Sept. 16, 2014).

[57] *Facebook Agreement*, *supra* note 51.

[58] *Id*.

[59] *Id.*; *see infra* notes 180–90 and accompanying text (removing a trusted connection and covertly replacing a company-substitute devalues the professional network).

[60] *LinkedIn Agreement*, *supra* note 46.

[61] *Id*.

[62] *Twitter Impersonation Policy*, TWITTER, https://support.twitter.com/articles/18366-impersonation-policy (last accessed Oct. 13, 2014).

[63] *See, e.g.,* Eagle v. Morgan, Civil Action No. 11–4303, 2013 WL 943350, at *11 (E.D. Pa. Mar. 12, 2013) (refuting the employer's claims of account for two reasons: there was no written corporate policy

suggested that a company can seize control of an employee's personal social media account if a written company policy or employment contract makes this practice explicit.[64]

¶27 While the duty of the court is often to balance the interests of the parties, when unequivocal provisions of a binding contract (between the user and SNS) are ignored, one might assume that the contract is either not pertinent or that the language of the agreement is unclear. Yet these contracts unmistakably give not only exclusive-access rights to the individual members,[65] but also openly manifest the impermissibility of account transfers.[66] Why courts seem to give employment contracts more credence than the SNS contracts is unclear, especially considering the totality of the circumstances discussed *infra* Part VII(c). This Comment therefore turns to why courts and commentators have chosen to grant such little weight to SNS agreements. The most relevant case—*Eagle v. Morgan*—best illustrates both the contractual asymmetries and legal confusion surrounding social media in this context.

III. *EAGLE V. MORGAN*: JUDICIAL DEFERENCE FOR EMPLOYERS

A. Facts and Holding

¶28 The defendant, Edcomm Inc. (Edcomm), took control of a former chief executive's LinkedIn account following her involuntary termination.[67] Dr. Eagle, the former president and cofounder of the recently acquired Edcomm, had created a LinkedIn account in 2009, which she used to promote the company, foster her reputation in the banking industry, and build a network of personal and professional contacts.[68]

¶29 After the acquisition, Edcomm's new management team promulgated a revised social media policy.[69] Management urged all employees to create LinkedIn accounts, and suggested the material that should be included in employees' profiles, but did not explicitly require employees to create accounts, and never paid for LinkedIn's "Premium" services.[70] Importantly, Edcomm never memorialized this policy in writing.[71] Nevertheless, Edcomm believed it retained the right to claim ownership of an employee's LinkedIn account upon termination.[72] Edcomm concluded that this practice was

---

mandating this practice and "the LinkedIn User Agreement clearly indicated that the individual user owned the account"); Phonedog v. Kravitz, No. C 11–03474 MEJ., 2011 WL 5415612, at *4 (N.D. Cal. Nov. 8, 2011) (acknowledging that "Phonedog has adequately alleged that it owns or has the right to possess the account" after receiving testimony that Twitter's terms stated otherwise).

[64] *See Eagle*, 2013 WL 943350, at *16.

[65] *See LinkedIn Agreement*, *supra* note 46 (emphasis added) ("You agree to: . . . not sell, trade, or *transfer* LinkedIn account to another party.").

[66] See *Eagle*, 2013 WL 943350, at *16, for dicta suggesting that the company may have been able to assert ownership over Dr. Eagle's LinkedIn account if an explicit, written corporate policy existed stating such a company practice.

[67] *See Eagle*, 2013 WL 943350, at *2.

[68] *Id.* at *1.

[69] *Id.*

[70] *Id.*

[71] *See id.*

[72] *Id.*

permissible if they replaced a former employee's name and identity with the new account holder's information.[73]

¶30 Immediately following Dr. Eagle's termination, Edcomm seized control of her LinkedIn account.[74] Edcomm allegedly instructed Dr. Eagle's former assistant, who had helped Dr. Eagle manage her social media accounts, to sign into her account and change the password.[75] While a few identifying features were not deleted, such as Dr. Eagle's awards and recognitions, Edcomm personnel changed the name on the account and position held to match the new CEO's identity.[76] Dr. Eagle quickly realized she could no longer access her account and that the identifying information had changed, which led to the eventual lawsuit.[77]

¶31 The court held that Dr. Eagle failed to meet her burden of proof against Edcomm for identity theft, tortious interference with contract, conversion, civil conspiracy, and aiding and abetting.[78] However, the court found that Edcomm had used her name without authorization in violation of Pennsylvania law, misappropriated her identity, and tortiously invaded her privacy.[79] But the court did not award compensatory damages because Dr. Eagle was unable to show any specific, quantifiable financial loss in the three weeks without access to her account.[80] Further, because the court felt that Edcomm could have reasonably inferred that they were acting lawfully, it found that punitive damages were similarly unjustified.[81]

¶32 The court attempted to mesh traditional common law doctrines and state statutes to form the basis for its decision. Because she was well known in the banking industry, the company had violated Dr. Eagle's right of publicity when it used her LinkedIn account for commercial gain.[82] Moreover, if someone had searched online for Dr. Eagle during the exclusion period, instead of finding her, the Internet user would have found her replacement.[83] Among other reasons, the fact that Edcomm benefited from Dr. Eagle's name and reputation led the court to determine that Edcomm wrongfully seized Dr. Eagle's LinkedIn account.[84]

---

[73] *Id.*
[74] *Id.* at *3.
[75] *Id.*
[76] *Id.* A previous court had granted summary judgment in favor of Edcomm for Dr. Eagle's claims under the CFAA and the Lanham Act. Eagle v. Morgan, Civil Action No. 11–4303, 2012 WL 4739436, at *9 (E.D. Pa. Oct. 4, 2012), *aff'd*, Eagle v. Morgan, Civil Action No. 11–4303, 2013 WL 943350 (E.D. Pa. Mar. 12, 2013). The court dismissed the CFAA claim because "potential business opportunities" were too "speculative . . . [and] not compensable under the CFAA." *Id.* at *5. The court dismissed the Lanham Act claims because the changed account did not create confusion as to the identity of the account holder. *Id.* at *7. Rather, while an Internet search led those looking for Dr. Eagle to her replacement, the confusion only resulted as to how the user found her replacement. *Id.* And since Edcomm changed the identifying information, Edcomm did not try to "pass off" Dr. Eagle as still an employee at Edcomm. *Id.*
[77] *Id.* at *6.
[78] *Id.* at *17.
[79] *Id.*
[80] *Id.*
[81] *Id.* at *15.
[82] *Id.* at *8.
[83] *Id.*
[84] *Id.*

¶33 Most important for this Comment, the court in *Eagle* suggested, *inter alia*, but for the absence of a written policy specifically asserting the right to take the social media account, the company could have prevailed.[85] Subsequent commentary has identified this factor—the lack of an explicit statement asserting company ownership of employee social media accounts—as the foundation for restrictive social media policies. In addition to such social media policies, many suggest that courts are more likely to enforce these employment provisions if certain conditions are met, such as whether:

> (1) the employer paid the . . . fees; (2) the employer dictated the precise terms of the employee's account; (3) the employee acted expressly on behalf of the employer due to her position, role, or responsibility; [and] (4) the social media account was developed and built through investment of the employer's time and resources.[86]

While these factors were merely alluded to in dicta, they support the increasingly popular opinion that an explicitly restrictive social media policy mitigates the risk of future litigation and allows companies to maintain access to and control over individual-member social media accounts.[87] Ultimately, if companies take heed and adopt these suggestions, more and more employees will lose a valuable professional resource upon termination.

B. Criticism: Common Law Application and Damages Rationale

¶34 *Eagle v. Morgan* exemplifies the unsettled relationship between social media and the law. The court rightfully relied on recent precedent and traditional legal doctrines to reach its holding. However, the result is seemingly contradictory.[88] Edcomm intentionally violated the law to gain a commercial advantage to Dr. Eagle's detriment, yet Dr. Eagle recovered no damages because she could not prove actual loss during the time Edcomm wrongfully excluded her from the account.[89] Moreover, although the facts are somewhat unclear, Dr. Eagle was unable to retrieve any messages from the time Edcomm had control of her account.[90] Keeping in mind that Dr. Eagle's LinkedIn profile was often the only means for clients to contact her,[91] for Dr. Eagle to recover damages, she needed to show—with certainty—that an individual wishing to complete a transaction was unable

---

[85] *Id.*

[86] Wayne Chang & Paul Cowie, *Who Owns Your Online Persona?*, 18 CYBERSPACE LAW. 7, 7 (2013). "The lesson [from *Eagle*] is clear: Employers wishing to protect social media accounts which they view as company marketing and branding should act now and introduce clear policies regarding ownership." *Id.*

[87] *See* Jodka, *supra* note 8, at 1 (suggesting companies draft clear corporate policies that assert ownership over all social media accounts used in relation to employment and that employee access will cease upon termination); Kasarjian, *supra* note 22, at 20 (suggesting employers draft specific contracts because "[i]t is important to note at the outset who owns and has a right to view/use information, communications, and even accounts—such as LinkedIn").

[88] *Eagle*, 2013 WL 943350, at *17 ("[T]he outcome of this case results in somewhat of a mixed bag for both sides.").

[89] *Id.*

[90] *Id.* at *3.

[91] *Id.* at *4 (discussing how 70% of Dr. Eagle's average annual sales came from existing contacts).

to contact her through LinkedIn sometime during the twenty-four days that she was excluded from the account.[92] This is like asking a man without a telephone to prove how many phone calls he has missed.

¶35 Specifically, the court's comparison of social media to dissimilar technologies shows the inherent challenges associated with the application of archaic doctrines to novel innovation. For instance, the court rightfully asserted that conversion claims in Pennsylvania only apply to tangible chattels or intangible chattels that can be "merged in, or identified with, a single document."[93] In turn, the court categorized the LinkedIn account as something similar to software, domain names, and satellite signals, all of which are intangible chattels not subject to conversion.[94]

¶36 But these comparisons are problematic. The court focused on examples involving the wrongful taking of sharable technology, which if used by many people concurrently, only marginally diminishes the chattel's value, if at all.[95] For instance, the *Eagle* court cited *Apparel Business Systems*, *LLC v. Tom James Co.*, which dealt with the wrongful copying of software, to justify finding that a LinkedIn account, like software, qualifies as an intangible chattel not subject to conversion.[96] Yet the copying of software does not preclude the rightful owner from using or selling the product, whereas the loss of access to Dr. Eagle's account eliminated her ability to receive benefits stemming from her reputation and identity on LinkedIn.

¶37 Further, while social media users often share information publically, only the SNS and individual licensee have the right to access an account.[97] This confers the right to exclude others. The licensing agreement explicitly grants exclusive, inalienable access rights, and clearly defines a contractual relationship between only the individual user and the SNS.[98] In other words, the intangible chattel (the LinkedIn account) could "be merged in, or identified with" the SNS user agreement—a single document.[99] Unlike inexhaustible satellite signals[100] or transferable domain names,[101] SNS agreements grant individual users the exclusive right to exclude others from accounts solely attributed to that user's identity. However, these inapt comparisons were the court's only options because, realistically, social media's use in the workplace and its attendant value is unprecedented.

---

[92] *Id.* at *13.

[93] *Id.* at *10 (quoting Giordano v. Claudio, 714 F. Supp. 2d 508, 524 (E.D. Pa. 2010)).

[94] *See id.*

[95] *See, e.g.,* Robert D. Haymer, *Who Owns the Air: Unscrambling the Satellite Viewing Rights Dilemma*, 20 LOY. L.A. L. REV. 145, 151 (1986) (describing satellite signals as technically inexhaustible).

[96] *Eagle*, 2013 WL 943350, at *10 (citing Apparel Bus. Sys. v. Tom James Co., Civil Action No. 06–1092, 2008 WL 858754, at *18 (E.D. Pa. Mar. 28, 2008)).

[97] *See, e.g., Facebook Agreement*, *supra* note 51; *LinkedIn Agreement*, *supra* note 46; *Twitter Terms*, *supra* note 45.

[98] *See, e.g., Facebook Agreement*, *supra* note 51; *LinkedIn Agreement*, *supra* note 46; *Twitter Terms*, *supra* note 45.

[99] *Eagle*, 2013 WL 943350, at *10.

[100] *See* Haymer, *supra* note 95 (comparing satellite signals to wild animals).

[101] *See Introduction to Buying and Selling Domain Names*, PCNAMES.COM, http://www.pcnames.com/Articles/An-Introduction-to-Buying-and-Selling-Domain-Names (last visited Feb. 28, 2014); *cf. LinkedIn Agreement*, *supra* note 46 (forbidding transfer or sale of accounts).

¶38 In addition, the court refused to award compensatory damages because Dr. Eagle was unable to prove that Edcomm's actions caused her to lose any specific clients. In the weeks following her termination, when Dr. Eagle lost access to her LinkedIn account, she could not identify any individuals who were looking for her online and unable to find her.[102] Instead, Dr. Eagle relied on a retroactive formula that used the average amount of revenue generated through her LinkedIn network to calculate a loss of between $248,000 and $500,000.[103] The court found this evaluation too uncertain.[104] Dr. Eagle also failed to prove a causal link between the average loss and the defendant's actions.[105]

¶39 While requiring a "reasonable certainty" of damages is a well-established legal maxim, requiring Dr. Eagle to identify specific transactions to recover damages ignores the complexities of social media's commercial value. In many ways, social media's value is analogous to the value of traditional advertising. Ordinarily, an advertiser cannot track revenue generated from a single advertisement.[106] Companies normally measure an advertisement's value not in actual revenue, but through more holistic methods.[107] For instance, "effective advertising frequency" evaluates the amount of times a consumer views an advertisement and how that frequency correlates to an eventual purchase.[108] Similar methodologies look at how exposure indirectly leads to financial gain.[109] Thus, analogous to social media networks, an advertisement's value stems from repeated, long-term exposure—not specific, identifiable transactions.[110] In this context, the more a user actively interacts with her online community, the higher the likelihood for economic gain. The widespread and recurrent interaction through social media can be highly valuable, yet at the same time mostly unquantifiable, which makes the *Eagle* court's requirement that Dr. Eagle identify the loss of specific transactions highly prejudicial.

¶40 Simply stated, how could Dr. Eagle realistically show this loss if she could neither access her account nor retrieve past messages? The court reasoned that if someone really wanted to contact her, the Internet user would have "sought out other ways to reach her."[111] But what if someone initially tried to communicate with her, and after no

---

[102] *Eagle*, 2013 WL 943350, at *13.

[103] *Id.*

[104] *Id.*

[105] *Id.*

[106] *See* Robert Bruce, *Traditional Advertising Is Truly Dead*, COPYBLOGGER, http://www.copyblogger.com/advertising-is-dead/ (last updated Mar. 24, 2013, 9:46 AM).

[107] *See, e.g.,* Roy Williams, *How to Track Ad Results*, ENTREPRENEUR, http://www.entrepreneur.com/article/159392 (last visited Aug. 26, 2014); Phil Fernandez, *4 Ways Marketers Can Drive Revenue—and Prove It*, FAST CO. (Jan. 10, 2012, 12:05 AM), http://www.fastcompany.com/1807078/4-ways-marketers-can-drive-revenue-and-prove-it.

[108] *See* Molly Elmore, *The Effect of Repeated Exposure to Advertising over Time*, INSIGHT EXPRESS, https://www.insightexpress.com/docs/default-source/white-papers/the-effect-of-frequency-over-time.pdf?sfvrsn=2 (last visited Oct. 19, 2014) ("When planning media in a digital environment, frequency of exposure has long been known to be an important variable.").

[109] *See id.*; *cf.* Eric Clemons, *Why Advertising Is Failing on the Internet*, TECH CRUNCH (Mar. 22, 2009), http://techcrunch.com/2009/03/22/why-advertising-is-failing-on-the-internet/ (describing advertising that allows for "experience and participation in a virtual community" as the most effective form of online advertising).

[110] *See* 3 ALLAN D. WINDT, *Advertising Injury Coverage*, *in* INS. CLAIMS AND DISPUTES § 11:29 (6th ed. 2014) (describing "advertising injury" as incorporating elements of unfair competition and invasion of privacy).

[111] Eagle v. Morgan, Civil Action No. 11–4303, 2013 WL 943350, at *14 (E.D. Pa. Mar. 12, 2013).

response, decided to take his business elsewhere? In a saturated marketplace, where companies increasingly vie for a larger slice of the pie, is the intentional and wrongful elimination of a resource that has a longstanding, revenue-generating track record not enough of a hindrance to justify at least a "reasonably fair basis" for recovery?[112] Ultimately, *Eagle* illustrates the unique intersection of social media and the law, which often requires solutions that do not exist within traditional legal frameworks.

IV. PRIVACY & PUBLICITY RIGHTS: SUPPORT FOR EMPLOYEE RIGHTS

¶41 Forced-transfer provisions implicate privacy concerns and the common law right of publicity. Regarding privacy, while social media usage is inherently public, certain aspects of an individual-user account, such as the ability to send and store messages, retain a very personal quality. However, courts and lawmakers have been reluctant to address privacy in the workplace, especially when new technology is involved.[113] At first blush, the court's analysis of whether Edcomm invaded Dr. Eagle's right of privacy provides the best judicial guidance. In the end, though, privacy law falls short.

¶42 Part IV first explores the origin and evolution of the right of privacy. This provides helpful background for an analysis of Dr. Eagle's "successful" claims, the *Eagle* court's application of various common law doctrines, and ultimately, privacy law's failure to provide adequate guidance in this context. Part IV concludes by evaluating the expectation of privacy generally.

A. The Right of Privacy in Eagle

¶43 The right of privacy is a relatively new concept.[114] Published in 1890, Samuel Warren and Louis Brandeis's seminal article—*The Right of Privacy*—first described this interest as the right "to be let alone."[115] More than half a century later, William Prosser built upon Messrs. Warren and Brandeis's analysis when he divided privacy interests into four separate categories.[116] Almost all states have adopted Prosser's categories, often codifying them as distinct torts.[117] Common law has expanded upon these interests, creating new causes of action under "the rubric of privacy."[118] However, applying this right and defining its contours has proven difficult.

¶44 The Pennsylvania Supreme Court recognized a cause of action for invasion of privacy by appropriation of name or likeness in 1976.[119] Pennsylvania also recognizes a

---

[112] *Id*. at *13.

[113] *See infra* Part IV(b). *See generally* Stratton, *supra* note 17 (discussing the constitutional right to information privacy with regard to public employees' social media login information).

[114] Melvin v. Reid, 297 P. 91, 93 (Cal. Dist. Ct. App. 1931).

[115] Louis D. Brandeis & Samuel D. Warren, *The Right of Privacy*, 4 HARV. L. REV. 193 (1890).

[116] *See* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

[117] *See* Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1904 (2010).

[118] *Id.* at 1907.

[119] *See* Vogel v. W. T. Grant Co., 327 A.2d 133 (Pa. 1974); *see also* Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 562 (1977) (recognizing the distinction between the *right* of publicity tort and the traditional invasion of privacy tort).

cause of action for invasion of privacy by misappropriation of publicity.[120] But while the right of publicity technically falls within the bounds of privacy law, it "may be regarded as the reverse side of the coin of privacy."[121] As such, the right of publicity has been defined as "the right to control the commercial use" of an identity, focusing on the value misappropriated rather than any harm done to a "person's mental psyche."[122] This distinction is due to the nature of the right of publicity[123] and the lack of traditional legal norms to protect "an axiom of the most fundamental nature, that every person is entitled to the fruit of his labors unless there are important countervailing public policy considerations."[124]

¶45 Like many states, Pennsylvania codified the right of publicity with a commercial-advantage requirement. Thus, for a claimant to meet her burden of proof, she must show that the wrongful act was committed for commercial gain.[125] In contrast, the tort of invasion of privacy by misappropriation of name or likeness does not require that a claimant prove a "commercial benefit."[126] The court in *Eagle* recognized these two distinct torts and held that Edcomm had violated both.[127] Yet Edcomm's culpable behavior did not lead to financial repercussions.[128]

¶46 In this context, the damages assessment in *Eagle* prohibitively weakened privacy protection. Referring to the fact that individuals searching for Dr. Eagle would unknowingly be led to her replacement, the court stated that "[s]uch a scenario could be deemed to be 'appropriat[ing] to [Edcomm's] own use or benefit the reputation, prestige, social or commercial standing, public interest or other values of plaintiff's name.'"[129] However, although misappropriation of name or likeness protects an interest more akin to a property right,[130] the court focused only on Dr. Eagle's inability to show any specific lost profits. Yet for nearly twenty-four days, Dr. Eagle's replacement benefitted from the exposure of the professional network that Dr. Eagle had built.[131] As discussed previously, similar to advertising, Edcomm profited from the indirect, repeated contact with Dr.

---

[120] *Compare* 42 PA. CONS. STAT. § 8316 (2003), *and* BLACK'S LAW DICTIONARY (9th ed. 2009) (defining "Invasion of Privacy by Appropriation" as "protect[ing] one's property right to the economic benefits flowing from the commercial use of one's face or name"), *with* Lewis v. Marriott Int'l, Inc., 527 F. Supp. 2d 422, 429 (E.D. Pa. 2007) (rejecting the argument that "the cause of action for invasion of privacy by misappropriation of identity has been 'subsumed' by [§] 8316" in that it still does not require the misappropriated use to be commercial).

[121] Melvin B. Nimmer, *The Right of Publicity*, 19 L. & CONTEMPORARY PROBLEMS 203 (1954), *reprinted in* NIMMER ET AL., CASES AND MATERIALS ON COPYRIGHT AND OTHER ASPECTS OF ENTERTAINMENT LITIGATION INCLUDING UNFAIR COMPETITION, DEFAMATION, PRIVACY 1249 (8th ed., 2012).

[122] Thomas Phillip Boggess V, *Cause of Action for an Infringement of the Right of Publicity*, *in* 31 CAUSES OF ACTION 2d 121 (2006).

[123] *See* Nimmer, *supra* note 121, at 1257 (describing right of publicity as "the right of each person to control and profit from the publicity values which he has created or purchased").

[124] *Id*.

[125] *See* 42 PA. CONS. STAT. § 8316 (2003).

[126] *See* RESTATEMENT (SECOND) OF TORTS § 652C cmt. a (1977) ("[T]he right created by it is in the nature of a property right, for the exercise of which an exclusive license may be given to a third person, which will entitle the licensee to maintain an action to protect it.").

[127] *See* Eagle v. Morgan, Civil Action No. 11–4303, 2013 WL 943350, at *11 (E.D. Pa. Mar. 12, 2013).

[128] *See id.* at *17.

[129] *Id.* at *8.

[130] *See* § 652C cmt. a.

[131] *See Eagle*, 2013 WL 943350, at *8.

Eagle's online community. In other words, Edcomm's culpable behavior resulted in unjust enrichment, albeit indirectly, from the use of Dr. Eagle's account; an account founded upon valuable personal connections effectuated by Dr. Eagle's identity and corresponding reputation.[132] In sum, Edcomm benefited from both the court's ill-fitted damages requirement and the complexities of social media's commercial value in the workplace.

¶47 Although some privacy rights recognize the inherent value in an individual's name and reputation, imposing such a high threshold for certainty of damages likely precludes recovery for most claimants in this context, even after proving a clear privacy violation. A social media account is not an interactive website for consumers to purchase a product. Nor is it an email account that clients may send official documentation identifying a purchase.[133] Social media is a medium of personal expression that allows individuals to interact. Dr. Eagle lost this potential for interaction because Edcomm wished to insert itself into her online community.

¶48 In the end, privacy protection falls short. The difficulty in proving with certainty that direct, identifiable damages resulted from the defendant's conduct realistically precludes plaintiffs from recovering damages for the loss of access to social media accounts. And because the interest protected is similar to a property right, it is fully licensable, which negates its applicability when an employment contract explicitly grants these rights to an employer.[134]

B. The Expectation of Privacy in Social Media

¶49 The U.S. Supreme Court recently eschewed a similar issue when asked to determine whether an employer violated an employee's expectation of privacy when the employer searched through personal text messages on an employer-provided pager.[135] Recognizing the difficulty in determining privacy rights in an evolving technological landscape, the Court stated that these expectations "will be shaped by those changes or the degree to which society will be prepared to recognize those expectations as reasonable."[136] Thus, while the Court's reluctance to address workplace privacy leaves questions unanswered, its acknowledgment that privacy rights are determined by societal expectations leaves our issue within the purview of the lower courts.

¶50 Courts need to ask whether a reasonable employee would expect to lose her social media account upon termination. For instance, as qualified *supra*,[137] if a company hires an employee to manage its social media platforms, and the employee creates accounts in the name of the company, then that employee should not reasonably expect to retain access to those accounts upon termination. However, when an employee uses her

---

[132] *See supra* notes 106–10 and accompanying text.

[133] *Cf.* AFL Phila. LLC v. Krause, 639 F. Supp. 2d 512, 518 (E.D. Pa. 2009) (holding that defendant's wrongful use of former employee's email address caused reputational damage).

[134] RESTATEMENT (SECOND) OF TORTS § 652C cmt. a (1977).

[135] Patricia Sánchez Abril, Avner Levin & Alissa Del Riego, *Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee*, 49 AM. BUS. L.J. 63, 65 (2012) (citing City of Ontario, Cal. v. Quon, 560 U.S. 746 (2010)).

[136] *Id.*

[137] *See supra* note 39 and accompanying text.

individual-member account for business purposes, her privacy expectations may reasonably change, especially given the nebulous relation between the social and professional use of social media.[138] And even if an employee signed a contract that included a forced-transfer provision, the equitable considerations in the employer/employee context discussed *infra* Part VII(c) support the idea that social media accounts created in her name and associated with her identity are nevertheless inalienable.[139]

V. TRADE-SECRET LAW: MORE THAN JUST AN ELECTRONIC ROLODEX

¶51 In contrast, while individual social media accounts prompt some privacy concerns, they are inherently a very public mode of self-expression. Yet some commentators have looked to trade-secret law for solutions.[140] In other words, an employer might assert ownership of employee social media accounts following termination by claiming that these accounts and the attendant networks qualify as trade secrets, and thus belong to the company.[141] While trade-secret law varies across states, "any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others," broadly defines what typically constitutes a trade secret.[142] This expansive definition includes any information that could provide a competitive advantage that falls outside copyright or patent protection.[143]

¶52 But information that is industry knowledge or "readily ascertainable" falls outside trade-secret protection.[144] The information does not need to be technical for trade-secret protection, but must not easily derive from public information.[145] For instance, the Supreme Court of Georgia described trade-secret law as a means of protecting employer property.[146] Specifically, the Georgia Court held that a departing employee has the right

---

[138] *See* Cosentino, *supra* note 29; Brutocao, *supra* note 30.

[139] See Abril et al., *supra* note 135, at 108, for a survey conducted of mostly 18–24 year olds, where "Millennial respondents displayed a clear discomfort with the idea of information flowing across contexts. Three-fourths found it inappropriate for an employer to check employee off-duty conduct via social networks. More than half (56%) objected to the practice of social media background checks."

[140] *See, e.g.,* Jasmine McNealy, *Who Owns Your Friends?:* Phonedog v. Kravitz *and Business Claims of Trade Secret in Social Media Information*, 39 RUTGERS COMPUTER & TECH. L.J. 30 (2013).

[141] *See id.*

[142] *Id.* at 34 (quoting RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995)). *See* UNIF. TRADE SECRETS ACT § 1(4) (amended 1985) ("Trade Secret means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.").

[143] McNealy, *supra* note 140, at 34–35.

[144] *See id.*; Jodka, *supra* note 8 (describing how the public nature of social media negates trade secret protection because trade secrets "must be (1) maintained in confidence, (2) have commercial value from not being generally known, and (3) not be readily ascertainable by proper means").

[145] *See, e.g.,* Eagle v. Morgan, Civil Action No.11–4303, 2011 WL 6739448, at *9 (E.D. Pa. Dec. 22, 2011), *aff'd*, Eagle v. Morgan, Civil Action No. 11–4303, 2013 WL 943350 (E.D. Pa. Mar. 12, 2013); *see also* Jodka, *supra* note 8.

[146] *See* Avnet, Inc. v. Wyle Labs., Inc., 437 S.E.2d 302, 304 (Ga. 1993).

to take all knowledge gained during employment, information not belonging to the employer, and that customers (not being property) are not trade secrets.[147]

¶53 Further, when an employee expends a significant amount of effort in creating a client list, and the employer allows the employee to maintain the list throughout employment, courts are less likely to find the existence of a trade secret.[148] Identifying where this relationship exists, whether between the employee or the employer and the customer list, is essential to typical trade-secret-protection analysis.[149]

¶54 With rare exceptions,[150] individual social media accounts should fall outside the scope of trade-secrets law.[151] First, much of the value associated with a professional network stems from the very public nature of the relationship.[152] Finding that these user accounts are eligible for trade-secret protection seems entirely antithetical to social media's purpose in the workplace. Simply stated, professional networking requires public exposure.[153] Second, unlike someone responsible for managing a public page in the name of a company, the individual user is solely responsible for building and maintaining her professional network.

¶55 Social media's value arises from the relationships existing amongst a professional network. As discussed *infra* Part VII(a), the quality of these connections likely enhances social media's value more so than the quantity. Although a user's account can function like a rolodex, storing and organizing beneficial contact information, the interactive nature of social media distinguishes it from a client list, which is potentially subject to trade-secret protection. When someone initiates contact through social media, the individual accepting the request does so believing that he or she is connecting with the employee, not the employer. In sum, these relationships exist between individuals, not companies, which removes professional networks from the ambit of trade-secret protection.[154]

---

[147] *Id.*

[148] *See* Jenifer A. Maygar, *Protecting Company Information from Ex-Employees*, FINDLAW (Mar. 26, 2008), http://corporate.findlaw.com/litigation-disputes/protecting-customer-infromation-from-ex-employees.html (citing Robert S. Weiss Inc. & Assocs. v. Wiederlight, 546 A.2d 216, 224 (Conn. 1988)) ("Connecticut courts have found that employees in a particular industry know what public resources to consult in order to identify their customers, and therefore, courts do not consider customer information a trade secret.").

[149] *See id.*

[150] *See* McNealy, *supra* note 140, at 37–45. Looking to some common exceptions, if an account's privacy settings are strict, the client list is significantly detailed, and the employer shows that adequate time and resources were expended by the company in establishing and protecting the list, a social media account could arguably fall within the protection of trade-secrets law. *Id.*

[151] *See, e.g.,* Sasqua Grp., Inc. v. Courtney, No. CV 10–528(ADS)(AKT), 2010 WL 3613855, at *9 (E.D.N.Y. Aug. 2, 2010) (discussing how the public nature of the LinkedIn network removes it from trade-secret protection); *see also* Jodka, *supra* note 8 (referring to a British court that held a LinkedIn network was a trade secret similar to a protected client list).

[152] *See* McNealy, *supra* note 140, at 50.

[153] *See, e.g., LinkedIn Agreement*, *supra* note 46 (describing LinkedIn as the world's largest professional network).

[154] *See* McNealy, *supra* note 140, at 44 (describing court reasoning that identified the personal relationships between a former employee and past clients that removed future professional contact between the parties from trade-secrets protection).

VI. JUDICIAL AND LEGISLATIVE TRENDS: THE PROGRESSION OF SOCIAL MEDIA RIGHTS IN THE WORKPLACE

¶56 The decision in *Eagle* illustrates how established legal principles often fail to provide adequate solutions for disputes concerning new technology. However, subsequent commentary continuously attempts to identify old frameworks for these modern issues. For instance, recognizing the inapplicability of intellectual property law in this context, some have attempted to address social media access rights through the CFAA, a decades-old statute originally drafted to combat computer hacking.[155]

A. The Computer Fraud and Abuse Act (CFAA)

¶57 Some have identified the CFAA as a possible solution.[156] Originally enacted in 1986, Congress has amended the "anti-hacking" statute multiple times to "keep pace with technological development."[157] Providing for both a private right of action and potential criminal liability, Congress intended the CFAA to deter and punish hackers attempting to gain access to protected computers for economic gain.[158] Courts and Congress have expanded the CFAA's applicability to cover an employee who wrongfully accesses a company computer to gain an economic advantage.[159]

¶58 Additionally, since the CFAA applies to access rights, it more easily fits with social media ownership-rights analysis because there is no need to manipulate intellectual property law.[160] In other words, the fact that neither employer nor employee truly owns the account matters far less under the CFAA. Pertinent to our analysis, the CFAA states, "Any person who suffers damage or loss by reason of a violation . . . may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief."[161] Further, the CFAA broadly defines "loss" to include "any revenue lost, cost incurred, or *other consequential damages* incurred because of interruption of service."[162] Thus, at first blush, the CFAA appears to provide potential relief for claims similar to that of Dr. Eagle's.

¶59 However, the CFAA is less helpful in determining access rights for individual-member social media accounts. First, although the CFAA could arguably cover a situation where an ex-employee retains access to or changes the password of an account created in the name of the company, it is harder to justify its applicability to individual-member accounts. The crux of a CFAA claim is the extent to which the usage goes beyond the authorization granted to the employee by the employer.[163] Regarding

---

[155] *See* Miao, *supra* note 28.
[156] *See id.* at 1017.
[157] *Id.* at 1033, 1061; *see* 18 U.S.C. §§ 1001, 1030 (2012).
[158] *See* Miao, *supra* note 28, at 1033.
[159] See *id.* at 1024 for a discussion of Ardis Health, LLC v. Nankivell, No. 11 Civ. 5013(NRB), 2011 WL 4965172, at *3 (S.D.N.Y. Oct. 19, 2011), where an ex-employee hired to manage a company's social media account was ordered to return the login information to her former employer because the employer "own[ed] the rights to the Access Information."
[160] *Id.* at 1060.
[161] 18 U.S.C. § 1030(g) (2012).
[162] § 1030(e)(11) (emphasis added).
[163] *See id.*; Hernacki, *supra* note 26, at 1547–48 (arguing CFAA's scope should be limited to original

individual-user accounts, the agreement made between the SNS and the user defines this scope of authorization.[164] As the "exclusive owner" of the account, "individually bound" by the agreement, the user's right to access an account is paramount to all but the true owner's—the SNS.[165] Until an SNS deems otherwise, an employee is authorized to use that service, even if the employee violates the accepted terms of service.

¶60 Moreover, the CFAA has typically applied to situations where an employee takes proprietary information without permission.[166] But even if a company has effectively stored contact information within a company's protected computer system, it must have received that data from an individual user's social media account. And not only is the employee initially responsible for gathering this information, but also a professional network consists of people, not property, making the CFAA as analogously inapplicable as trade-secret law. In other words, these personal connections are anything but proprietary information.[167]

¶61 Discussed *supra* Part II, an SNS retains the right to suspend account access at its sole discretion. Although employees might use company computers to gain access to their accounts throughout the course of employment, only the SNS operates the platform, and the SNS user agreement defines the extent of user authorization.[168] Thus if the CFAA applies at all in this context, it is the SNS, not the company, that could pursue a private right of action against a user. However, as seen in *Eagle*, courts have increasingly applied a narrower interpretation of the CFAA, which requires an actual "hacking" violation and implies a more stringent threshold for recoverable damages.[169]

¶62 In this same vein, courts have begun to question the enforceability of the CFAA in employer-employee disputes, creating a circuit split.[170] In 2012, the Ninth and Fourth Circuit Courts interpreted the "exceeds authorized access" and "without authorization" language narrowly, pointing out that the purpose of the CFAA is to combat hacking, not to hold employees liable for any slight infringement of an employer's computer-use

---

legislative goal of drafting an "anti-hacking" statute).

[164] *See LinkedIn Agreement, supra* note 46 (asserting agreement is between the user and LinkedIn, notwithstanding the fact that a person may be acting on behalf of a company).

[165] *See id.*

[166] Miao, *supra* note 28, at 1054; *see, e.g.,* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 580 (1st Cir. 2001) (finding ex-employee, acting beyond his authority defined by a confidentiality agreement, violated the CFAA when he used a "scraper" to gather information from former employer's website); *see also* United States v. Phillips, 477 F.3d 215, 220 (5th Cir. 2007) (holding that unintended use of company's computer network, entirely unrelated to defendant's prior job function, amounted to a CFAA violation).

[167] *See* Thomas E. Booms, Note, *Hacking into Federal Court: Employee "Authorization" Under the Computer Fraud and Abuse Act*, 13 VAND. J. ENT. & TECH. L. 543, 560 (2011) ("[W]hile the presence of an employment agreement may bolster the company's case against a rogue employee, it is not dispositive."); *see also* Creative Computing v. Getloaded.com, LLC, 386 F.3d 930, 932 (9th Cir. 2004) (finding CFAA violation when defendant hired competitor's employee to login to plaintiff's protected website and download a confidential client list).

[168] *See supra* notes 97–98 and accompanying text.

[169] Eagle v. Morgan, No. Civ. 11–4303, 2012 WL 4739436, at *5 (E.D. Pa. Oct. 4, 2012) ("[Dr. Eagle] claims that she was denied potential business opportunities as a result of Edcomm's unauthorized access and control over the account. Loss of business opportunities . . . is simply not compensable under the CFAA."), *aff'd*, Eagle v. Morgan, No. Civ. 11–4303, 2013 WL 943350 (E.D. Pa. Mar. 12, 2013); *see* Mooney, *supra* note 31.

[170] *See* Cosentino, *supra* note 29.

policy.[171] Therefore, in these jurisdictions, the misuse of information by an employee will not meet the revised statutory threshold for civil liability if the employer gave the employee access to that information in the course of her employment.[172]

¶63 Although other circuits have yet to join the Fourth and Ninth Circuits, district courts in the Second, Third, Sixth, and Eighth Circuits have adopted this narrow interpretation "with the expectation that their respective circuits will follow."[173] Thus, following this judicial trend, the prospect of the CFAA assisting in the interpretation of social media ownership rights seems unpromising because of not only its unsettled state, but also the fact that courts are increasingly applying the narrower interpretation, as seen in *Eagle*.[174]

B. State and National Legislation

¶64 Recent legislative trends point to the increasing preference for employee privacy protection in social media. For example, six states—California, Delaware, Illinois, Maryland, Michigan, and New Jersey—have recently passed laws that prohibit employers from asking for social media passwords,[175] and analogous legislation has been introduced or is pending in twenty-eight states.[176] Similarly, § 7 of the National Labor Relations Act, which protects employees' rights to engage in protected, concerted activity, has provided relief for employees when an employer terminates or reprimands an employee because of certain statements made online.[177] Specifically, in a May 2012 memorandum, the National Labor Relations Board issued a statement extending § 7 protection for employees' social media usage.[178] With recent fears relating to privacy exacerbated by various controversies (e.g., the NSA's mass surveillance of phone records), nothing suggests that legislation geared towards protecting social media privacy rights is likely to cease.[179]

---

[171] Audra A. Dial & John M. Moye, *The Computer Fraud and Abuse Act and Disloyal Employees: How Far Should the Statute Go to Protect Employers from Trade Secret Theft?*, 64 HASTINGS L.J. 1447, 1450 (2013) (citing WEC Carolina Energy Solutions, LLC, v. Miller, 687 F.3d 199 (4th Cir. 2012) and United States v. Nosal, 676 F.3d 854 (9th Cir. 2012)).

[172] *See id.*; Mooney, *supra* note 31, at 16 ("Eagle's disclosure of her password to the employees, who later accessed her account using the authorized password, foreclosed any such [CFAA] claim."). *But see* NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1058 (S.D. Iowa 2009) ("The legislative history of § 1030(e)(6) supports the broad view.").

[173] *See* Dial & Moye, *supra* note 171, at 1457.

[174] Mooney, *supra* note 31.

[175] Kasarjian, *supra* note 22, at 21.

[176] *Employer Access to Social Media and Passwords*, NAT'L CONFERENCE OF STATE LEGS., http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx#2014 (last updated Sept. 28, 2014).

[177] *See* Kasarjian, *supra* note 22.

[178] *See id.*; Alyesha A. Dotson*, NLRB Outlines Employers' Social Media Policies Do's and Don'ts,* SPILLMAN, THOMAS & BATTLE P.L.L.C (Apr. 29, 2013), http://www.spilmanlaw.com/resources/attorney-authored-articles/labor---employment/nlrb-outlines-employers--social-media-policy-dos-a.

[179] *See* James Hendler, *It's Time to Reform the Computer Fraud and Abuse Act*, SCI. AM. (Aug. 16, 2013), http://www.scientificamerican.com/article/its-times-reform-computer-fraud-abuse-act/ (proposing a change to the CFAA's "draconian measures" following the suicide of Aaron Schwartz, an Internet activist who committed suicide after being charged with eleven felonies and up to thirty-five years in prison).

¶65 In sum, the inapplicability of traditional legal frameworks combined with these judicial and legislative trends protecting privacy rights create an opportunity to explore alternative guidelines. While most legal justifications further muddle social media rights analysis, the economic and social benefits of social media's use in the workplace are clear. Thus, perhaps an analysis focusing on these clear benefits provides instruction.

VII. SOCIAL MEDIA VALUATION: SOCIOECONOMIC RATIONALE

¶66 The proliferation of company policies that include forced-transfer provisions could substantially hamper social media's future value, both economically and socially. After balancing the equities, the negative socioeconomic impact of forced-transfer provisions should tip the scales in favor of an exclusive judicial rule proscribing this practice. Further, the potential for social media's devaluation should prompt SNSs to take action as well.

¶67 Part VII first argues that empirical evidence and various studies suggest that social media's potential financial and social value is not only intrinsically intertwined, but also wholly dependent on interpersonal connection. Because forced-transfer provisions insert unknown company representatives into these social networks, in the aggregate, over commercialization of these once-personal networks will stymie the sharing of ideas, hindering the corresponding growth of online communities. Part VII(b) next turns to SNS intervention, and specifically how SNSs can deter this deleterious practice from negatively affecting SNSs generally. Finally, Part VII(c) suggests that this adverse social impact should prompt courts to proscribe the enforceability of these overly restrictive provisions.

A. The True Value of Social Media: Online Communities Built on Trust

¶68 Social media's value in the workplace is undeniable. While over 72% of companies use social media, one study estimates that the potential economic value of social media is still largely untapped, with trillions of dollars in value unrealized.[180] According to the same study, the biggest challenge in capturing this added value is the difficulty in establishing workplace conditions that foster collaboration.[181] Only through work environments that encourage participation and embrace trust will communication within organizations and across enterprises lead to this potential growth.[182] Aligning with this concept, the first section of LinkedIn's User Agreement explains that the purpose of the social media platform is to allow people to create a "network of *trusted* relationships and groups."[183]

---

[180] *See* SOCIAL ECONOMY, *supra* note 6.

[181] *See id.* "The value contribution from improved communication, coordination, and collaboration—potentially two-thirds of all potential value from use of social technologies in business organizations—is embedded in these projections." *Id*. at 9. While this analysis includes all "social technologies," even by more conservative estimates, the potential commercial value of social media is significant. *Id.*

[182] *See id.*

[183] *LinkedIn Agreement*, *supra* note 46 (emphasis added).

¶69 Furthermore, LinkedIn's User Agreement prohibits members from soliciting unfamiliar connections, making it arguably the most restrictive of the popular SNSs.[184] Similarly, Twitter and Facebook explicitly and repeatedly forbid a user from creating accounts in someone else's name or misleading others as to his identity.[185] Unlike other areas of the Internet where anonymity flourishes, the personal accountability within a social media network creates an environment where users are free to develop and share ideas with trusted connections, thus allowing like-minded communities to form.[186]

¶70 In fact, many argue that the pitfalls of anonymity pose the biggest threat to successful online communities.[187] For instance, the over commercialization of the once-popular MySpace arguably caused its failure. Instead of providing a platform for communities to connect, "MySpace diverted its attention to serving eyeballs to advertisers and fell even more behind on facilitating the 'social' part of social networking."[188] In other words, SNSs that facilitate the free formation of trusted groups incent the sharing of ideas and the corresponding growth of the online community.[189]

¶71 Furthermore, a Cornell study found that the "tendency of an individual to join a community is influenced not just by the number of friends he or she has within the community, but also crucially by how those friends are connected to one another."[190] Therefore, in tandem with creating an environment of trust to foster collaboration, the potential economic value associated with social media's growth arguably depends not only on the amount of connections within a network, but also the quality of the connection among members.[191]

---

[184] *See id.*

[185] *See Twitter Terms*, *supra* note 45.

[186] *See* Boyd & Ellison, *supra* note 1, at 219 ("'[P]ublic displays of connection' serve as important identity signals that help people navigate the networked social world, in that an extended network may serve to validate information presented in profiles.").

[187] *See* JEREMY KEESHIN, SOCIAL NORMS ON THE WEB: HOW TO CREATE PRODUCTIVE DIGITAL COMMUNITIES 7 (2010), *available at* http://thekeesh.com/docs/norms.pdf ("There is a large anti-spam effort, because spam represents those trying to undermine the community with noise. [SNSs] institute policies to fight the shortcoming of online communities—mainly anonymity—but succeed in varying measures."); *see, e.g., Facebook Agreement*, *supra* note 51 ("You will not post unauthorized commercial communications (such as spam) on Facebook."); *LinkedIn Agreement*, *supra* note 46 (prohibiting spam and attempting to connect with and/or contact with people who do not know you or "who are unlikely to recognize you as a known contact").

[188] Chunka Mui, *Why Facebook Beat MySpace, and Why MySpace's Revised Strategy Will Probably Fail*, FORBES (Jan. 1, 2011), http://www.forbes.com/sites/chunkamui/2011/01/12/why-facebook-beat-myspace-and-why-myspaces-revised-strategy-will-probably-fail/; *see* Boyd & Ellison, *supra* note 1, at 22 ("[T]rust and usage goals may affect what people are willing to share—Facebook users expressed greater trust in Facebook than MySpace users did in MySpace and were thus more willing to share information on the site.").

[189] Mui, *supra* note 188 (describing "Reed's Law," developed by David Reed of the Massachusetts Institute of Technology, as the framework by which SNSs will flourish).

[190] LARS BACKSTROM ET AL., DEP'T OF COMPUTER SCI., CORNELL UNIV., GROUP FORMATION IN LARGE SOCIAL NETWORKS: MEMBERSHIP, GROWTH, AND EVOLUTION 1 (1976), *available at* http://www.cs.cornell.edu/~lars/kdd06-comm.pdf.

[191] *See id.* While this Cornell study focuses on offline behavior, many commentators point out the similarity of group behavior, whether online or not: "The idea that group dynamics and social interaction follow many of the same rules from offline is well supported." KEESHIN, *supra* note 187, at 3. Further, the saliency of a group—"the amount that users find the group to be self-defining, affects the adherence to communal norms." *Id.*

¶72 While most companies use social media, few have specific social media policies in place.[192] In fact, only within the past few years have social media policies become a focal point of corporate governance.[193] Because of this trend, if these forced-transfer provisions become a common and enforceable aspect of employment contracts, their adoption could extend quickly and expansively.[194] If this is the case, it will lead to the widespread transference of social media accounts from original users to company-appointed substitutes.[195] These substitutes will most likely not have personal connections with the majority of the network. In this same vein, because of the undeniable value stemming from these personal connections, there is a clear incentive for the employer to conceal or at least limit public communication of the account holder's changed identity. Therefore, while a network may not necessarily lose members, it may lose a portion of its potential value because the personal connection among members will fray.[196]

¶73 No longer will the purpose of social media be to create an environment for "trusted relationships" to form,[197] but one where companies may acquire large swaths of networks, substituting personal connections for data collection or some other commercial purpose.[198] Even though these companies might not be impersonating former employees, they will be substituting uninvited colleagues into an online community.

¶74 While this may seem hyperbolic, taking into account the increasing rate of career change among Millennials,[199] these policies could lead to the devaluation of social media,

---

[192] *See* Amy Gesenhues, *Survey: 71% of Companies Concerned over Social Media Risks, but Only 36% Provide Employee Training*, MKTG. LAND (Sept. 27, 2013, 3:28 PM), http://marketingland.com/survey-71-of-companies-concerned-about-social-media-risks-only-36-do-social-media-training-60212 (indicating that 33% of companies surveyed have a social media policy in place); Samuel Axon, *Most Companies Don't Have a Social Media Policy in Place*, MASHABLE (Feb. 3, 2010), http://mashable.com/2010/02/03/social-networking-policy/ (noting that 29% of companies in the Americas have a "formal policy" regarding social media use); *see also* Kasarjian, *supra* note 22.

[193] *See* Gesenhues, *supra* note 192.

[194] See *id.* for analysis of a survey which indicates that while 33% of company respondents had a social media policy in place, 27% had no social media in place and no plans to adopt one. Accordingly, showing the potential for widespread adoption of company social media policies, 40% of respondents had plans to create a social media policy in the near future, or had other related policies. *Id*.

[195] See Susan H. Stephan, *Datamining for Gold: Social Media and Social Capital in a Postnational Global Market*, 39 N. KY. L. REV. 163, 167–71 (2012), for a discussion of the potential for corporate and governmental interference in the global Internet community, namely the increasing corporate interest in privatizing the Internet. But compare, SOCIAL ECONOMY, *supra* note 6, at 12, for the proposition that consumers might benefit economically from data-mining in that "social technologies provide the insights that allow consumers to purchase goods that are better suited to their needs."

[196] *See* SOCIAL ECONOMY, *supra* note 6. The economic potential of social media depends on these trusted connections. *Id.* RICK LAWRENCE ET AL., SOCIAL MEDIA ANALYTICS: THE NEXT GENERATION OF ANALYTICS-BASED MARKETING SEEKS INSIGHTS FROM BLOGS 1 (2010), *available at* http://www.prem-melville.com/publications/sma-orms10.pdf ("In July 2009, a survey conducted by Universal McCann concluded that 31.7% of more than 200 million bloggers worldwide blog about opinions on products and brands, and that 71% of all active Internet users read blogs. The 2009 Nielsen Global Online Consumer Survey of 25,000 Internet users in 50 countries has found 70% of consumers trust opinions posted online by other consumers."); BACKSTROM ET AL., *supra* note 190.

[197] *See LinkedIn Agreement*, *supra* note 46.

[198] *See* LAWRENCE ET AL., *supra* note 196, at 26 (describing social media analytics as an emerging discipline where data-mining and other marketing strategies provide companies the opportunity to leverage social media to track consumer behavior).

[199] *See* Carl Bialik, *Seven Careers in a Lifetime? Think Twice Researchers Say*, NUMBERS GUYS BLOG (Sept. 4, 2010, 12:01 AM), http://online.wsj.com/news/articles/SB10001424052748704206804575468162

stymieing its growth and decreasing its utility through a steady attrition of reliable personal networks.[200] This could drastically affect not only a crucial form of networking for businesses, but could also lead to over-commercialization, prompting less usage and community participation.[201] Simply stated, the value of these networks is found not in the sheer number of members, but rather in the quality of connections fostered through social media's usage.

B. SNS Action: Time to Intervene

¶75 This potential economic degradation should prompt SNSs to take action. However, since these disputes primarily involve only the employer and employee, judicial intervention is also necessary. This section proposes that SNSs should draft user agreements explicitly banning the forced transfer of member accounts, and in the future, actively pursue legal claims for breach of contract when these forced transfers occur. Alternatively, SNSs should deactivate accounts that have changed owners. While the latter is not ideal in that social networks will lose some members, it negates the insertion of company representatives, thus remedying—albeit partially—the overall negative impact of these forced-transfer provisions.

¶76 First, although SNS user agreements currently forbid the transferring or selling of individual accounts, SNSs should expressly prohibit this employment practice, making judicial enforcement of these provisions less likely. Further, even if SNS user agreements explicitly prohibit the transfer of an account, the breach does not void the agreement.[202] In fact, since these licenses are revocable at the SNS's sole discretion, a court may hesitate to grant a user agreement significant weight when there has been a clear breach, but the SNS has not resorted to self-help.[203] After all, forced-transfer provisions violate the SNS's policies, and if the SNS is not actively enforcing the terms of its own agreement, then equitable intervention might be determined unnecessary.[204] Thus, SNSs should legally intervene to enforce the user agreements, further bolstering the legitimacy of the agreement between the SNS and the user. Up to this point, SNS involvement in

---

805877990.

[200] See KEESHIN, *supra* note 187, at 15, for a discussion of how honest representation benefits social media. For the successful development of an online community, "it is important that the users be attached and invested to their online identity, and that it is an accurate and honest representation of their self." *Id.*

[201] *Id.* Self-governing online communities flourish when members are connected to their identities thus allowing for accountability. *Id.* "If they become anonymous, then any iterated interactions or punishment is worthless because they create a new worthless account. A punishment to an anonymous user doesn't do anything, and this is why the foundation of a successful social norm system depends on legitimate identities." *Id.* at 14.

[202] *See LinkedIn Agreement, supra* note 46; *Twitter Terms*, *supra* note 45; *Facebook Agreement, supra* note 51.

[203] Courts often require plaintiffs to show that defendant's intentional inducement of the breach of the contract rendered performance impossible. Here, the SNS would have standing to sue, but would need to show actual damages. On the other hand, the employee would have to show not only damages, but also that the transfer of the account to the employer rendered performance impossible. *See* M. J. & K. Co. v. Matthew Bender & Co., 220 A.D.2d 488, 490 (N.Y. App. Div. 1995).

[204] *See* Eagle v. Morgan, Civil Action No. 11–4303, 2013 WL 943350, at *17 (E.D. Pa. Mar. 12, 2013) (identifying lack of quantifiable damages for loss of account access); *cf.* RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 70 (2011) (describing Doctrine of Laches as an affirmative defense barring equitable intervention).

these lawsuits has not been practical because the expense of litigation far outweighs any damages in an individual suit. But now, taking into account the negative effects of these policies in the aggregate, SNSs should be more willing to take action.[205]

C. Judicial Intervention: Forced-Transfer Provision Enforceability

¶77 Notwithstanding the fact that SNS user agreements prohibit the transfer of social media accounts, courts have implied that accounts are indeed alienable. Thus, a judge-made rule proscribing the enforceability of forced-transfer provisions stands as the most suitable remedy. However, this paternalistic stance, which contradicts traditional principles of contract law, requires justification found not in the text of these various contracts, but in equity. In other words, courts should balance the inherent socioeconomic asymmetries between the employer and employee to evaluate the fundamental fairness of restrictive social media policies. This Comment concludes that when employers knowingly induce employees to breach SNS user agreements, courts should acknowledge the unequal bargaining power between the parties, and thus equitably prohibit the enforcement of these agreements.

¶78 For instance, the employer's intentional interference with the SNS user agreement could be a basis for equitable intervention. When an employment contract compels account transference upon termination, the employer has induced the employee to breach his contract with the SNS. In many states, "intentional interference with performance of a contract by third person" applies when a party has improperly interfered with a contract or *prospective* contractual relation with another.[206] Thus, if an employee uses social media at the company's direction, this common law doctrine applies to the employer regardless of whether the employee created an account with an SNS before employment commenced. If the employment contract includes a forced-transfer provision, the employer intends for an employee to breach certain terms of an already existing, or soon-to-be formed, social media contract when that employee leaves the company.[207]

¶79 When deciding whether an action qualifies as intentional interference with contract, courts typically consider the relations between the parties and the "social interests in protecting the freedom of action of the actor."[208] First, a court should note the often-unequal bargaining power between a jobseeker and potential employer.[209] Second, the ex-employee would most likely suffer greater proportional harm by losing access to the professional network.[210] For jobseekers, it increases the likelihood of securing suitable

---

[205] *See supra* text accompanying notes 177–91.

[206] *See* RESTATEMENT (SECOND) OF TORTS § 766 cmt. g (1979); *see, e.g.,* Haddle v. Garrison, 525 U.S. 121, 126 (1998) (recognizing third-party interference claim with an employment contract as long established in tort law); Onyeoziri v. Spivok, 44 A.3d 279, 286 (D.C. 2012) (applying factors in RESTATEMENT (SECOND) OF TORTS § 766 for tortious intentional interference with contract claim).

[207] *See* RESTATEMENT (SECOND) OF TORTS § 766 (1979).

[208] RESTATEMENT (SECOND) OF TORTS § 767(e).

[209] *See* RESTATEMENT (SECOND) OF TORTS § 767(g); *see, e.g.,* Armendariz v. Found. Health Psychcare Servs., Inc., 6 P.3d 669 (Cal. 2000) (recognizing the unequal bargaining power between employer and employee in pre-employment contract negotiation); *see also* Franklin G. Snyder, *The Pernicious Effect of Employment Relationships on the Law of Contracts*, 10 TEX. WESLEYAN L. REV. 33, 34 (2003) (suggesting employment contracts deal more with questions of status, rather than contractual relations).

[210] *See* RESTATEMENT (SECOND) OF TORTS § 766; *see also* Herron v. State Farm Mut. Ins. Co., 363 P.2d

employment.[211] For the recently hired, it expedites the onboarding process.[212] Specifically, if a company unexpectedly fires an employee, and the newly terminated employee does not have an opportunity to collect necessary contact information stored within an account, the employee experiences the most acute harm, losing an invaluable professional resource for both successful subsequent employment and the newly unemployed individual's job search.[213]

¶80 The employer, on the other hand, typically has a larger pool of resources to draw from, along with other means, such as non-compete agreements, to protect its interests. Companies adopt these forced-transfer provisions because of both the desire for economic gain and the fear of economic loss. The provisions ensure that the company will maintain access to a potentially lucrative professional network, while reducing the likelihood of an ex-employee poaching prospective or existing clients.[214] In many ways, it functions very similarly to a standard, otherwise enforceable, non-compete agreement.[215] However, the existence of a conflicting contract changes the circumstances. Unlike a non-compete agreement where no prior contract exists, if an employee ever leaves the company, a forced-transfer provision inevitably leads to a breach of either the employment contract or the SNS user agreement.

¶81 Although the common law tort of intentional interference with contract varies across states, and often requires a showing of something similar to malice,[216] courts might be willing to extend the doctrine in this context pursuant to the judiciary's inherent equity powers. In sum, taking into account the equitable factors used by courts to determine liability for this tort, the nature of the employer-employee relationship, and the social ramifications associated with unemployment, a sympathetic court might choose to err in favor of employees' rights. Further, if SNS user agreements explicitly forbid this employment practice, courts may be even more likely to deem forced-transfer provisions unenforceable.

310, 312 (Cal. 1961) (balancing "the importance, social and private, of the objective advanced by the interference against the importance of the interest interfered with, considering all the circumstances including the nature of the actor's conduct and the relationship between the parties" to determine whether tortious intentional interference by a third-party occurred).

[211] *See* Susan Adams, *LinkedIn Still Rules as the Top Job Search Technology Tool, Survey Says*, FORBES (Aug. 12, 2013, 6:57 PM), http://www.forbes.com/sites/susanadams/2013/08/12/linkedin-still-rules-as-the-top-job-search-technology-tool-survey-says/ ("Social [m]edia sites like LinkedIn are the top way to search for candidates.").

[212] *See id.*

[213] *See id.*

[214] *See* Parent, *supra* note 8.

[215] *See, e.g.,* Teksystems, Inc. v. Bolton, Civil Action No. RDB–08–3099, 2010 WL 447782, at *5 (D. Md. Feb. 4, 2010) (discussing possible violation of former employee's non-compete agreement when he contacted clients through LinkedIn).

[216] *See* RESTATEMENT (SECOND) OF TORTS § 766 cmt. s (1979) ("There are frequent expressions in judicial opinions that 'malice' is requisite for liability . . . But the context and the course of the decisions make it clear that what is meant is not malice in the sense of ill will but merely 'intentional interference without justification.'"); *see, e.g.,* Hall v. FMR Corp., 667 F. Supp. 2d 185 (D. Mass. 2009); Louis Schlesinger Co. v. Rice, 72 A.2d 197, 202 (N.J. 1950) (citing Walker v. Cronin, 107 Mass. 555 (1871)) ("But if [the interference] comes from the merely wanton or malicious acts of others, without the justification of competition or the service of any interest or lawful purpose, it then stands upon a different footing.").

VIII. CONCLUSION

¶82 By adhering to the terms agreed upon between the individual user and the SNS, a blanket, judicial prohibition of these forced-transfer employment provisions will allow social media to reach its full economic and social potential. After balancing the equities, and taking into account established principles of contract, privacy, and tort law, the employee's right to retain social media account access must be assured through judicial intervention. Although federal legislation could achieve the same result, the judiciary's inherent equity powers give judges the discretion necessary to quickly and efficiently reach the most suitable solution.